Quick Reference Guide to Protected Distribution System (PDS) Implementation

Version 1.0
December 5, 2003

Introduction

Welcome to the PDS Reference Guide

What is a Protected Distribution System (PDS) and why should you be concerned? PDS is the system of carriers (conduits, ducts, etc) that are used to distribute National Security Information (NSI) between two or more controlled areas. Now, that answers the *what* but what about the *why*? That answer is two-fold. First, since PDS can be used in lieu of encryption, it may be more cost effective than installing COMSEC devices and secondly, it is a requirement when routing NSI along an area (I.e. passageway or room) that is controlled at a lower level of classification than the level of the NSI carried.

The complex made simple. The process for certifying existing PDS and installing new PDS is complex and requires coordination from multiple parties—and can take up to 209 days.

But, we have streamlined the process - Read more and learn.

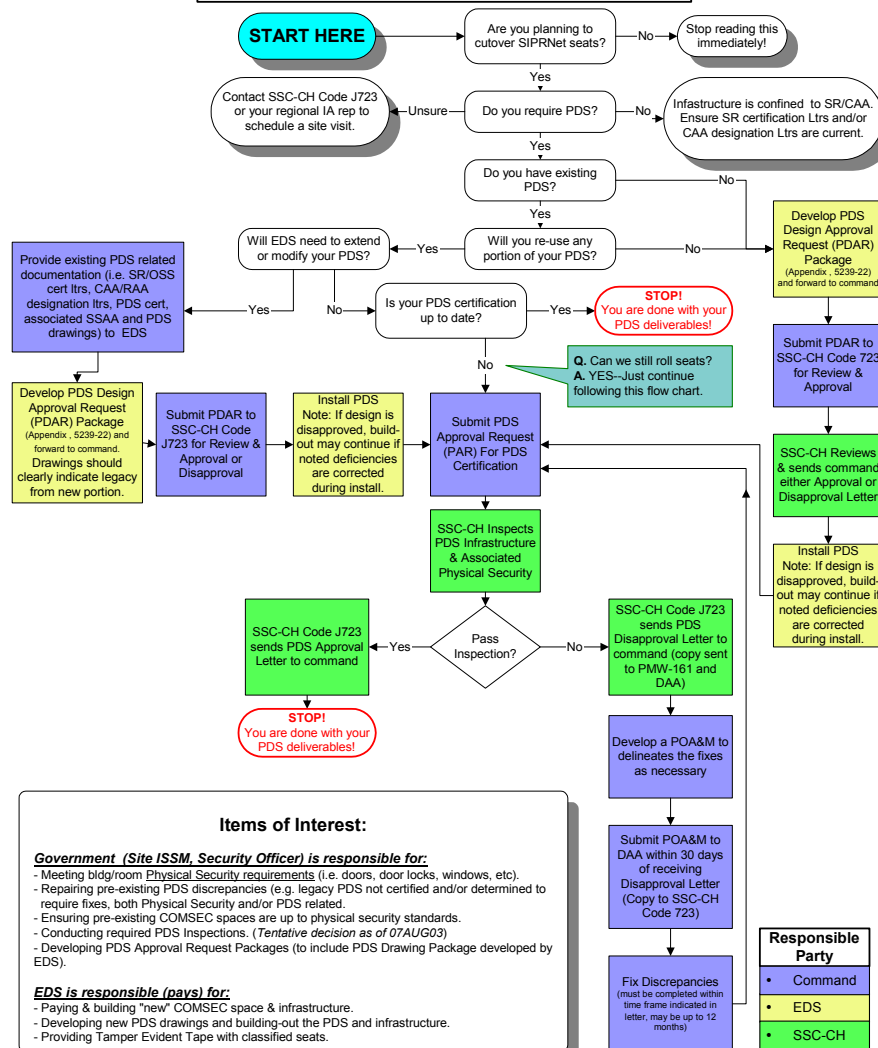STEP 1: Read the FAQ's
STEP 2: Go to the Master Flowchart

The Master Flowchart. Follow the master flowchart at the start button and just answer the questions to determine PDS requirements for your particular site.

Additional helpful information. For PDS Masters, go to page 6 for a quick reference. For PDS implementers go directly to page 7 for step-by-step instructions with detailed explanations, owners, listed references, templates and documents.

This guide is courtesy of the Southeast Region SITT IA Reps (KE/KR)

PDS FLOWCHART

PDS APPROVAL PROCESS FLOWCHART

START HERE

Are you planning to cutover SIPRNet seats? — No → Stop reading this immediately!

Yes ↓

Do you require PDS? — No → Infastructure is confined to SR/CAA. Ensure SR certification Ltrs and/or CAA designation Ltrs are current.

Unsure → Contact SSC-CH Code J723 or your regional IA rep to schedule a site visit.

Yes ↓

Do you have existing PDS? — No → Develop PDS Design Approval Request (PDAR) Package (Appendix , 5239-22) and forward to command

Yes ↓

Will you re-use any portion of your PDS? — No → (to Develop PDS Design Approval Request box)

Will EDS need to extend or modify your PDS? — Yes → Provide existing PDS related documentation (i.e. SR/OSS cert ltrs, CAA/RAA designation ltrs, PDS cert, associated SSAA and PDS drawings) to EDS

No ↓

Is your PDS certification up to date? — Yes → **STOP!** You are done with your PDS deliverables!

No ↓

Q. Can we still roll seats? **A.** YES--Just continue following this flow chart.

Provide existing PDS related documentation box → Develop PDS Design Approval Request (PDAR) Package (Appendix , 5239-22) and forward to command. Drawings should clearly indicate legacy from new portion.

→ Submit PDAR to SSC-CH Code J723 for Review & Approval or Disapproval

→ Install PDS Note: If design is disapproved, build-out may continue if noted deficiencies are corrected during install.

→ Submit PDS Approval Request (PAR) For PDS Certification

→ SSC-CH Inspects PDS Infrastructure & Associated Physical Security

→ Pass Inspection?

- Yes → SSC-CH Code J723 sends PDS Approval Letter to command → **STOP!** You are done with your PDS deliverables!

- No → SSC-CH Code J723 sends PDS Disapproval Letter to command (copy sent to PMW-161 and DAA) → Develop a POA&M to delineates the fixes as necessary → Submit POA&M to DAA within 30 days of receiving Disapproval Letter (Copy to SSC-CH Code 723) → Fix Discrepancies (must be completed within time frame indicated in letter, may be up to 12 months)

(Right column path from "Develop PDS Design Approval Request (PDAR) Package" top right):
→ Submit PDAR to SSC-CH Code 723 for Review & Approval → SSC-CH Reviews & sends command either Approval or Disapproval Letter → Install PDS Note: If design is disapproved, build-out may continue if noted deficiencies are corrected during install.

Items of Interest:

Government (Site ISSM, Security Officer) is responsible for:
- Meeting bldg/room Physical Security requirements (i.e. doors, door locks, windows, etc).
- Repairing pre-existing PDS discrepancies (e.g. legacy PDS not certified and/or determined to require fixes, both Physical Security and/or PDS related.
- Ensuring pre-existing COMSEC spaces are up to physical security standards.
- Conducting required PDS Inspections. (*Tentative decision as of 07AUG03*)
- Developing PDS Approval Request Packages (to include PDS Drawing Package developed by EDS).

EDS is responsible (pays) for:
- Paying & building "new" COMSEC space & infrastructure.
- Developing new PDS drawings and building-out the PDS and infrastructure.
- Providing Tamper Evident Tape with classified seats.

Responsible Party	
•	Command
•	EDS
•	SSC-CH

Q. We have an existing (legacy) PDS, what must be done if we want to connect our new NMCI classified seats to it? Do we need to get it re-certified?

A. **It depends. You can connect NMCI classified seats to previously certified PDS if the PDS certification is still valid (which means there were NO additions, extensions, and/or modifications after receiving the cert without informing SSC-CH). If you have a certified legacy PDS but it was in any way modified after receiving the cert, then SSC-CH needs to look at it to see if re-cert is required. Finally, if your legacy PDS is not certified, it <u>must</u> go through the certification process. Based on the severity of discrepancies noted (if any) a process is in place to provide connectivity while allowing you 12 months to fix discrepancies.**

Q. If EDS extends our existing PDS in order to accommodate additional classified seats ordered for the site, who is responsible for the design and installation of the PDS?

A. **EDS is responsible for the design and installation of new PDS (ref NMCI Contract), this includes PDS drawing development. Government is responsible for the physical security standards and requirements (Ref NMCI Contract).**

Q. After EDS reviewed our existing PDS they decided it would be more effective to install all new PDS. What process must they follow?

A. **IA-Pub 5239-22 01OCT03 Protected Distribution System (PDS) Installation Publication outlines the steps required to design, install and certify all PDS, regardless of who installs the system. EDS must adhere to DOD/DON regulations and will follow the same process as any other Navy or Marine Corps Command installing/certifying their PDS.**

Frequently Asked Questions (cont.)

Q. We do not need new PDS installed for our cutover, however, our current PDS is not certified. What action do we need to take?

A. **The process to use existing PDS requires you to provide a PDS certification document. If your command does not have one, your site ISSM submits a PDS Approval Request (PAR) Letter to SSC-CH (SPAWARSYSCEN Charleston Code 723, P.O. Box 190022 North Charleston, SC 29419-9022). To expedite the process include any existing (current) PDS drawings.**

Q. What can be done to speed up the PDS approval process?

A. **1) Start early. This cannot be emphasized enough. If issues arise, escalate them immediately.**

2) Develop communications with other key players involved with this process (Site Transition Manager, EDS rep, PDS Inspector, local IA rep). Cooperation will greatly accelerate this phase of pre-cutover and take you one step closer to meeting your cutover deadline.

3) Be proactive. Several things you can do are:

- **Identify personnel to support EDS site surveys**

- **Identify classified seats in existing secure areas**

- **Identify secure facilities**

- **Provide existing certifications (CMS, PDS, Controlled Access Area (CAA), COMSEC closets, etc.)**

- **Provide existing network documentation/drawings**

Q. If we plan to install new PDS, and our design is modified after a PDS Design Approval Request (PDAR) has been approved, do we have to resubmit a PDAR?

A. **No. Resubmission of the entire PDS Design Approval Request (PDAR) package is not necessary. If a site has already received a design approval letter and intends to modify their PDS design, an approval request for the design modification must be submitted. Requests for approval of a design modification to an approved PDS design may include only the items pertaining to the modification. Design modification approval requests may be sent in email format to the Certifying Authority (CA), SSC-CH, and should reference the approved PDAR. If the design modification is approved, then updated drawings should be included in the PDS Approval Request (PAR) package, and submitted after build out is complete. Information Systems Security Managers (ISSMs) are encouraged to contact the CA for guidance whenever a design modification is required.**

Q. Who is responsible for certifying rooms or buildings as Controlled Access Areas (CAAs) or Restricted Access Areas (RAAs)?

A. **The Information Systems Security Manager (ISSM) or Security Manager may designate a room or building a CAA or RAA by drafting a designation letter (template provided on the SPAWAR INFOSEC website). No formal certification is required for CAA/RAA designation, but implementation of physical security and room/building design shall comply with guidance set forth in IA-Pub 5239-22, "PDS Installation Publication" (01OCT03).**

Q. What if PDS is also required?

A. **If PDS is required at a site, the PDS Certifying Authority (CA), SSC-CH, validates LAA, RAA, and CAA designations as part of the PDS approval process. If no PDS is required because all classified data lines are within a CAA or Secure Room, then the Designated Approval Authority, NETWARCOM, validates that the areas meet the physical security and access control requirements per IA-Pub 5239-22. If an entire building is to be designated a CAA or RAA, it is recommended that the PDS CA be contacted for guidance in ensuring proper protection of information resources.**

Frequently Asked Questions (cont.)

Q. Our current PDS certification is a bit outdated and any existing discrepancies are minor. Additionally, we have not had any security incidents during it's operation. Can we get a waiver to use our current PDS as is?

A. **No. There are no permanent waivers for PDS (NMCI DAA, OPNAV, SSC-CH coordinated response). One of the main advantages of the NMCI initiative is strict adherence to network security policy. In order for that to occur, all sites must adhere to the same requirements prior to cutover. There is a process in place that allows a period up to 12 months for full compliance. Sites that have had their legacy PDS disapproved should submit a SSC-CH PDS Inspector approved POA&M and the disapproval letter to NETWARCOM within 30 days of receiving a disapproval letter from SSC-CH.   The POA&M should address all discrepancies identified in the disapproval letter. If additional time is required to generate a POA&M, the site should request an extension from NETWARCOM.**

Q. Who pays for what with regard to PDS?

A. **The Government is responsible for repairing pre-existing PDS discrepancies and ensuring all physical facility infrastructure is compliant. This includes ensuring pre-existing COMSEC closets are up to physical security standards.**

EDS is responsible for building out new PDS and building/providing <u>new</u> COMSEC closet infrastructure.

Q. If EDS installs new PDS for our site, who is responsible for the required inspections, Government or EDS?

A. **PDS inspections are a responsibility of the Government.**

PDS Approval Process (high level)

NMCI
NAVY MARINE CORPS INTRANET

Steps

Develop PDS Design Documentation

Submit Approval Request For Design Approval

Install PDS

Submit Request For Approval

Generate POA&M and submit to DAA - or - **Receive Final PDS Approval from DAA**

Allows up to 12 months without full compliance to correct the discrepancies in legacy PDS.

Purpose

Identify classified seat requirements, existing PDS and new ISF's PDS Template drawings

Avoid costly revisions and/or unnecessary installations

Complete PDS build-out

Obtain approval to roll classified seats

Roll/Connect classified seats

Step 1 – Develop PDS Package

Develop PDS Design Documentation

Tips For Success
PDS design should be coordinated early in the NMCI infrastructure build-out

Step No.	Action	Responsible Parties
1.	Provide <u>existing</u> PDS related documentation (secure room cert, PDS cert, SSAA and PDS drawings) to assigned EDS rep. SSC-CH is available for existing PDS Certs, related information, and/or potential Site assists.	ISSM & Physical Security Manager
2.	Verify locations of requested classified seats are feasible (physical security restrictions may not permit requested location).	ISSM, Physical Security Manager & STM
3.	Obtain NMCI Classified Seat requirements based on submitted order.	Assigned EDS rep
4.	Develop PDS design based on classified seat locations and physical security specifications (based on current & potential upgrades). SSC-CH PDS rep is available for design assistance also.	Assigned EDS rep (coordinate w/ ISSM and Physical Security Manager)

Responsible Party ➡	Command	EDS	SSC-CH	PDS Quick Reference Guidev1.0 05 December 2003

Develop PDS Design Documentation (Cont)

Step No.	Action	Responsible Parties
5.	Develop PDS design package (based on EDS's PDS Design Template For Classified Processing Environments For Navy/Marine Corps Intranet (NMCI).	Assigned EDS rep/team
6.	Develop PDS Design Approval Request form (IAW NAVSO P-5239-22, App C). This shall include EDS's PDS Drawing Package and PDS Checklist). Check with SSC-CH for current form versions.	ISSM (in coordination w/assigned EDS rep)

Step 2 – Request Design Approval

Submit Approval Request For Design Approval

Tips For Success
PDS design packages should be accurate and as complete as possible to prevent delay

Step No.	Action	Responsible Parties
1.	Submit completed PDS Design Approval Request Package to SSC-CH (SPAWARSYSCEN Charleston Code 723, P.O. Box 190022 North Charleston, SC 29419-9022) with the following required information (as per ref NAVSO P5239.22 Appendix C) ▪ PDS Drawings (EDS developed) ▪ Completed PDS Installation Checklist (ref EDS's PDS Design document) ▪ Completed PDS Physical Security Checklist (ref EDS's PDS Design document)	ISSM, Physical Security Manager
2.	Perform technical/design review for approval/disapproval (note: PDS packages should be approved before beginning installation to avoid potentially costly revisions and/or unnecessary installation.	SSC-CH 723 rep (as assigned)

Step 3 – Install PDS

Install PDS

Tips For Success
Contact SSC-CH if design changes must be made during the installation phase, to ensure continued compliance

Step No.	Action	Responsible Parties
1.	Install PDS as described in the approved design package.	EDS Rep
2.	Perform periodic reviews during PDS installation to verify installation is in accordance with the approved design.	ISSM, Physical Security Manager & EDS PDS POC

Step 4 – Request PDS Approval

Request PDS Approval

Tips For Success
Prevent Delay! Ensure PDS Approval Request is as complete and accurate as possible

Step No.	Action	Responsible Parties
1.	Submit final PDS Approval Request Letter to SSC-CH (SPAWARSYSCEN Charleston Code 723, P.O. Box 190022 North Charleston, SC 29419-9022). Include any red-lined PDS drawing changes if applicable.	ISSM & Physical Security Manager
2.	Inspect PDS and provide results to Site and PMW-161.	SSC-CH 723 rep (as assigned)

Responsible Party ➡	Command	EDS	SSC-CH	PDS Quick Reference Guidev1.0 05 December 2003

Step 5 – PDS POA&M

NMCI

NAVY MARINE CORPS INTRANET

Develop POA&M for PDS
(REQUIRED IF PDS WAS DISAPPROVED AND DISCREPANCIES EXIST**)**

Tips For Success
• Do not delay on the POA&M
•Coordinate with all parties involved to ensure discrepancies are corrected.

Step No.	Action	Responsible Parties
1.	Develop a POA&M that delineates the fixes as appropriate: i.e. discrepancy, repair, repair date, responsible POC. Should only apply to legacy PDS discrepancies.	ISSM & Physical Security Manager (coordinate with EDS and SSC-CH)
2.	Submit POA&M to Commander, Naval Network Warfare Command (Attn: N64), copy PMW 161. IMPORTANT: POA&M should normally be submitted NO LATER THAN 30 days after a PDS disapproval letter is received. Requests for extensions should be submitted to NETWARCOM.	ISSM
3.	Monitor progress of POA&M	Site POCs, PMW-161, DAA, SSC-CH

Responsible Party ➡	Command	EDS	SSC-CH	PDS Quick Reference Guidev1.0 05 December 2003

Step 6 – Final PDS Approval

Receive Final PDS Approval

Tips For Success

• Maintain good records of all security documents, to include: secure room/CAA cert, PDS cert, SSAA and PDS drawings

Step No.	Action	Responsible Parties
1.	Provide final PDS approval to site, NMCI DAA, and PMW-161	Approval Authority (SSC-CH)
2.	Maintain permanent record of final PDS certification/approval.	ISSM, PMW-161

Miscellaneous Information

❑ **There are NO permanent PDS waivers**

- All discrepancies must be fixed within 12 months of receiving the PDS Disapproval letter.

❑ **Legacy (certified) PDS can be re-used.**

- If a certified legacy PDS has been modified, SSC-CH determines if re-cert is required.

❑ **Legacy (non-certified) PDS must get certified prior to re-use.**

- Command must submit a Local NMCI Legacy PDS Status letter with the PDAR.

- Command must submit a PDS Mitigation POA&M within six weeks of receiving the PDS Disapproval letter.

❑ **EDS is responsible (pays) for:**

- Pay/build "new" COMSEC closet infrastructure.New PDS drawing development, PDS build-out and infrastructure build-out.Provide Tamper Evident Tape with classified seats.NMCI SSAA development

❑ **Government (Site/Site ISSM, Security Officer) is responsible and/or pays for:**

- Meeting bldg/room Physical Security requirements (i.e. doors, door locks, windows, safes for classified removable hard drives, etc).

- Legacy/existing COMSEC Closets must meet required security specsRepair pre-existing PDS discrepancies (e.g. legacy PDS not certified and/or determined to require fixes, both Physical Security and/or PDS related).

- To ensure pre-existing COMSEC Closets are up to physical security standards.

- Conduct required daily PDS Inspections. *(Not yet confirmed as of 08Aug03)*

- Responsible to develop PDS Approval Request Letter (to include PDS Drawing Package developed by EDS).

❑ **SPAWAR PMW-161:**

- CTTAs certify PDS

Points of Contact

NETWARCOM

Deputy DAA	Cathy Baber	(757.417.6767)	cathy.baber@navy.mil
Action Officer (N64)	LT Hal Empson	(757.417.6776 x1)	hal.empson@navy.mil
NMCI IA Lead (N64BT)	Bob Turner	(757.417.6776 x2)	bob.turner@navy.mil
NMCI IA Support	Bill Hildenbrand	(757.417.6776 x3)	bill.hildenbrand@navy.mil

NNSOC

Global ISSM	CWO2 Avalyn Smith	(757.963.1045)	avalyn.smith@navy.mil

SPAWAR PMW 164 & PMW 161

PMO Classified Lead	CAPT Charles Braun	(619.524.7481)	charles.braun@navy.mil
Tech Solutions	Scott Henderson	(619.524.7597)	scott.henderson@navy.mil
Dept PM	Garnet Smith	(619.524.7334)	garnet.smith@navy.mil
C&A/ST&E	CDR John Sicklick	(619.524.7340)	john.sicklick@navy.mil
PMO PDS Liason	Robert Hannah	(619-725-5326)	robert.hannah@2asc.com

EDS/Raytheon

Classified Process	Matt Castelli	(703.736.4134)	matthew.castelli@eds.com
IA Transition C&A Manager	Brian Wolstencroft	(703.284.4327)	brian_J_wolstencroft@raytheon.com
Transition Manager	Allen Streitman	(727.302.4248)	allen_I_streitman@raytheon.com

DCMS

COMSEC Closet Certs	Haywood Royal	(202.764.2873)	

SSC CH PDS Inspectors

NMCI PDS/PM	Larry Leverette	(843.218.4493)	larry.leverette@navy.mil
NMCI PMO CTTA	Cody Crawford	(619.221.1419)	crawforc@spawar.navy.mil
Certified TEMPEST Technical Authority (CTTA)	Andy Fisher	(757.558.5209)	fishera@spawar.navy.mil
NMCI Classified Cert Agent	Jeff Sweeney	(843.218.4282)	jeff.sweeney@navy.mil
Hawaii Region	Glenn Ching	(808.554.2263)	gching@spawar.navy.mil

Site Integration Transition Team (SITT) IA Regional Reps

Northeast Region(includes National Capital)	Meghnad Konai	(301.693.6165)	konai_meghnad@bah.com
Southeast Region	Kelly Eda	(757.445.5729)	keda@att.com
Southeast Region	Kristine Reed	(757.445.5737)	kristinereed@att.com
Southwest Region	Coral Cook	(619.322.7382)	cook_coral@integrits.com
Northwest/Hawaii Regions	Tiffany Gerstmar	(760.802.6706)	tgerstmar@rlphillips.com

References

COMNAVNETWARCOMINST 5239.1, 25 Oct 02

Title: Navy Marine Corps Intranet (NMCI) Information Systems Security Personnel Roles And Responsibilities

https://info.nnsoc.navy.mil/nmci/policy/NETWARCOM5239.doc

SECNAV Instruction 5510.36, 17 March 1999

Title: Department of the Navy (DON) Information Security Program (ISP) Regulation

http://neds.nebt.daps.mil/551036.htm

IA PUB-5239-22, Oct 2003

Title: Information Assurance (IA) Protected Distribution System (PDS) Publication, Oct03

https://infosec.navy.mil/documents

EDS's Protected Distribution System (PDS) Design Template For Classified Processing Environments For Navy/Marine Corps Intranet (NMCI), 14 May 03

http://www.nmci.navy.mil/Primary_Areas/I_A_Security/Files/PDS_Design_Template.pdf

- Developed in coordination with EDS, SSC-CH, PMW 161, and PMO
- Incorporates OPNAV PDS requirements, PDS design process, and approved hardware / equipment information